IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 1, 2019, accepted May 1, 2019, date of publication May 9, 2019, date of current version May 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2915938

Disrupting Terrorist Networks Based on Link Prediction: A Case Study of the 9–11 Hijackers Network

ZHENDONG SU[1], KAIJUN REN[2], RUOYUN ZHANG[3], AND SUO-YI TAN[2,3]

[1]School of Management, University of Science and Technology of China, Hefei 230026, China
[2]College of Computer and College of Meteorology and Oceanology, National University of Defense Technology, Changsha 410073, China
[3]College of Systems Engineering, National University of Defense Technology, Changsha 410073, China

Corresponding authors: Kaijun Ren (renkaijun@nudt.edu.cn) and Suo-Yi Tan (tansuoyi_cn@outlook.com)

This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB0203801, and in part by the National Natural Science Foundation of China under Grant 61572510 and Grant 71871217.

ABSTRACT Relationships between terrorists are amorphous, invisible, distributed, and dispersed. The information on these networks is often incomplete and even erroneous. The key to disrupting the terrorists' network is to find the critical nodes whose removal will lead to network collapse, and however, most of the previous studies are based directly on the observed networks while neglecting an important fact that the observed networks may be incomplete. In this paper, we address the terrorist network disintegration problem based on link prediction. An effective method is proposed to find the critical nodes by the assistance of a link prediction algorithm. We make a case study of September 11th hijackers to illustrate our method. Five different disintegration strategies are applied to validate our method. The result shows that, with no more than 40% magnitude of missing information, by using the link prediction method to recover partial missing relationships information, our method can improve the network disintegration performance remarkably. Besides, we find that when the size of missing information is not too much, our method even outperforms than the results based on complete information. We refer to this phenomenon as the ''comic effect'' of link prediction, which means that the original network has been reshaped through the addition of some links by link prediction. As a result, the reshaped network is like an exaggerated but characteristic comic of the original one, where the important parts are emphasized.

INDEX TERMS Terrorist network, network disintegration, link prediction, network analysis.

I. INTRODUCTION

Terrorism is an extreme behavior caused by misunderstanding and ineffective communication between groups, ethnic or countries, which makes serious harm to society [1]–[3]. Since the start of this century, terrorist activities have occurred more frequent and rampant around the globe. The 2001 plane hijackings in the United States that killed some 3000 people, and the 2004 Madrid train bombings in Spain that killed 190 people and made some 1500 civilians injured. In 2005, a series of bombing in the most popular tourist destinations Bali made a huge negative impact on visitors, while the 2008 terrorist attacks in the financial center Mumbai seriously hindered its economic development. We were all shock by kinds of tragic events. As covert organizations, they are amorphous, invisible, distributed and dispersed. It is very important to attack and disrupt them for making our nation safer.

The disintegration strategy of terrorist organization network has been the focus of attention in the academic community for a long time, which has experienced a tremendous growth since September 11^{th} attack [4]–[7]. With social network analysis (SNA) introduced [8]–[10], the terrorist organization can be abstracted into networks according to the relationship between staffs themselves [11], staffs and network resources, skills and tasks [3] or staffs and their locations [12]. SNA introduced both visual and mathematical analysis to staffs relationships, such as, centrality [13], betweenness [14], closeness [15], which indicates various roles of nodes in a network, for example, leaders, gatekeepers, followers and facilitators, etc. These network analysis measures can help us gain a better view of terrorist networks

The associate editor coordinating the review of this manuscript and approving it for publication was Sabu M. Thampi.

in revealing importance and vulnerabilities of nodes. Many disintegration strategies and models have been provided based on staff relationship network model. Husssain [16] estimate the extent of information damage, the network function destroy and the technical support loss to evaluate the attack result. Wiil *et al.* [18] and Memon *et al.* [19], [20] gives the disruption strategy to removing key targets based on network centrality, location centrality, and network efficiency. Carley [20] estimates the different performance of network after key staffs deleted. Lefebvre *et al.* [21] provides a strategy based on the sequence theory to evaluate the disintegration extent of terrorist organization.

In the early works on network disintegration, due to the difficulty in collecting and accessing reliable data, previous studies of terrorist network usually used unreliable data sources such as news stories and media-generated incident databases, or assumed that the decision maker can obtain the perfect information on the network structure [22]–[26]. However, the perfect information on the network structure is not always available in many realistic cases, especial in terrorist networks. As for the terrorist attack, we may catch many suspects but we have to interrogate them one by one to get their relationship for capturing the structure of their organization, which is usually costly and even infeasible. It inspires us to focus on an important and frequent scenario of imperfect information, i.e., the information of partial links is missing which means we get the targets but we do not know the whole relationships. If we could predict and recover some missing relationships, it will save the cost of inquiry and guide us in understanding the link mechanism of terrorist networks.

As a data mining process, link prediction aims at estimating the likelihood of the existence of a link based on observed links and the attributes of nodes, which has emerged as an invaluable tool in many branches of modern information science [27]–[32]. Many algorithms have been proposed based on different theory, including Markov chains, similarity-based indices, statistical models, maximum likelihood methods and probabilistic models [28]. Considering the node attributes are generally hidden in the terrorist network, it may fail for some algorithms which based on node attributes. Thus, we employ the structural similarity algorithms, which is based solely on the topology structure of network.

In this article, we introduce link prediction as a guideline for attackers to improve the effect of network disintegration when facing the missing information scenario. The rest of this article is structured as follows. In Sec.II, we will present the mathematical description of link prediction and then propose a terrorist network disintegration model with incomplete link information based on link prediction, then we proved the validity of the model through numerical simulations in Sec.III. We firstly compare twenty link prediction algorithms and choose one suitable for the September 11^{th} hijackers network, and analyze the impact of link prediction on effect of network disintegration. Furthermore, we validate our method in other different disintegration strategies. Finally, conclusions and discussions are presented in Sec.IV.

II. MODEL OF DISINTEGRATION OF TERRORIST NETWORKS BASED ON LINK PREDICTION

Considering the relationship between staffs, a terrorist network formalized in terms of a simple undirected graph $G = (V, E)$, where V is the set of staffs (nodes), and E is the set of relations between staffs (links). Multiple links and self-loops are not allowed. Let $N = |V|$ and $W = |E|$ be the number of nodes and number of links, respectively. Let d_i be the degree of node v_i, where the degree of a node is the number of links connected to the node.

Assume that all nodes are known but information of partial links is missing. Denote by E_O the set of links which can be observed and E_M the set of missing links, respectively. Therefore, $G_O = (V, E_O)$ is the observed network. Clearly, we have $E_O + E_M = E$, and we define $\alpha = |E_M|/W (\in [0, 1])$ as the magnitude of missing link information. Denote by $E_U = V \times V$ the universal set which has the whole $N(N-1)/2$ possible links. Obviously, link prediction is a technique to infer the invisible part based on the knowledge of observed part, and we employed it to recover the missing links from E_M. Denote by $\Omega_P = E_U - E_O$ the space of link prediction, and denote by $E_P \subseteq \Omega_P$ the set of predicted links. Therefore, through adding predicted links from E_P, $G_P = (V, E_O \cup E_P)$ is the improved network. Denote by the ratio $\beta = |E_P|/|E_O|$ as the magnitude of additional link information. Due to the inaccuracy of link prediction, $E_P \neq E_M$. Denote by $E^+ = E_P \cap E_M$ the set of links that are predicted rightly. The mathematical diagram for link prediction problem in Fig.1 illustrates the description of link prediction intuitionally.

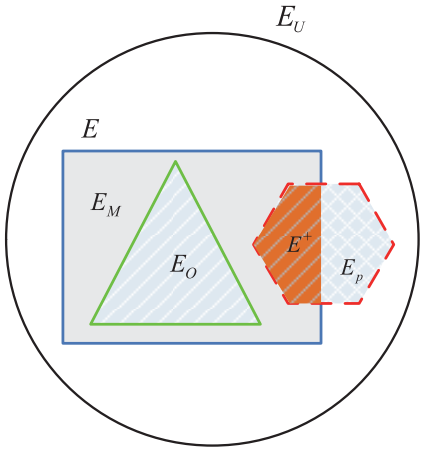

FIGURE 1. Mathematical diagram for link prediction problem. The rectangle represents the set of links E, i.e., the complete information, which is divided into two parts: The triangle is the observed part E_O, the rest of the rectangle is the invisible (missing) part E_M. The hexagon represents the set of predicted links, namely E_P. The polygon filled by stripes represents the set of links that are predicted right, namely E^+. The circle represents the universal set containing all possible links E_U.

Assume that once a target is attacked (i.e., captured or killed), all relationships of the target are cut off. Thus, We consider the node attack approaches in this study and assume that the attached links are removed if the node is attacked. Denote by $\hat{V} \subseteq V$ the set of nodes that are attacked (i.e., targets) and $\hat{E} \subseteq E$ the set of the attached links (i.e., relationships). Then we obtain the network $\hat{G} = (V - \hat{V}, E - \hat{E})$ after attacks. Denote by the ratio $f = \left|\hat{V}\right|/N \in [0, 1]$ as the strength coefficient of node attacks. There are many alternative attack strategies [33]. Here the most common ''degree centrality strategy'' was used to identify the leaders in the September 11^{th} network, i.e., high degree nodes indicate high levels of activity and wide influence, which means the hijackers with high degrees are likely to be the leaders of the network. It will be attacked firstly.

Denote by $\hat{d}_i$ be the degree of node v_i in G_O and denote by $\tilde{d}_i$ be the degree of node v_i in G_P. With the assistance of link prediction, we remove nodes in the descending order of the node degree $\tilde{d}_i$, and we compare this disintegration effect with the operation that removes nodes in the descending order of the node degree $\hat{d}_i$ directly based on the observed network G_O. To measure the disintegration effect in detail, we apply the measure R [24], [34], which evaluates the size of the largest connected cluster during the malicious attack on nodes. As the attack strength coefficient f increases, the network will eventually collapse. The smaller the R is, the more efficient disintegration effect is. The definition of R is

$$R = \frac{1}{N+1} \sum_{Q=0}^{N} S(Q) \tag{1}$$

III. EXPERIMENTAL RESULTS

A. DATA DESCRIPTION

The September 11^{th} incident was a series of coordinated attacks against the United States and thousands of innocent people were killed [11]. In this article, we applied our method on the September 11^{th} hijackers network as a case study of the terrorist network, which contains 62 nodes and 153 links. A node represents a terrorist, and a link between two terrorists shows that there is a social relation between the two terrorists, which includes friendship and co-participating in training camps or previous attacks. Our visualization provides an intuitive and clear view of the overall September 11^{th} hijackers network (See Fig.2). For example, Mohamed Atta (the largest yellow node), the leader of the central member clump, had 33 links to other hijackers and ranked the first in degree.

B. LINK PREDICTION METHODS

The simplest framework for link prediction is the similarity-based algorithm, where each pair of nodes, x and y, is assigned a score S_{xy}, denoting the similarity between them. All non-observed links are ranked according to their scores, and the links connecting more similar nodes are assumed to have higher likelihoods of existing. In this study, in order to choose a suitable index for September 11^{th} hijackers network, we evaluated twenty different similarity-based algorithms, which are classified according to three categories: nine local similarity indices, three global similarity indices, six quasi-local indices, and two other similarity-based indices. More details of these algorithms were given a previous review [28].

The AUC and precision accuracies of these methods on September 11^{th} hijackers network are shown in Table 1. In the experiment, the training set contains 90% of links, and the remaining 10% of links constitute the probe set. As for precision, empirical analysis shows that L usually ranges

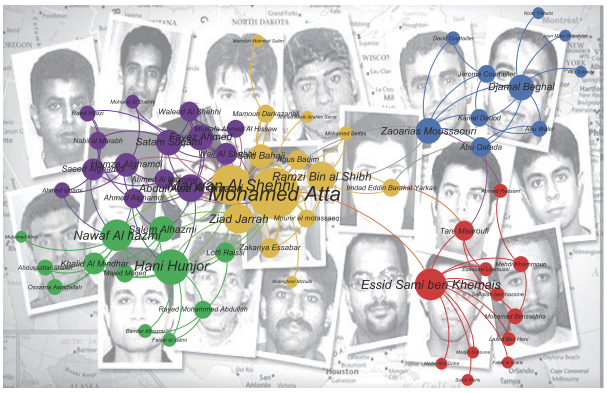

FIGURE 2. September 11^{th} hijackers terrorists network. Each node represents a terrorist, and link connected by two terrorists means they have a direct relationship. The size of the nodes is proportional to their degree value, the color of nodes is proportional to different airplanes hijacked based on the modularity algorithm provided by Lambiotte [35].

TABLE 1. Algorithmic accuracies of twenty different indices based on the September 11^{th} hijackers network measured by AUC and precision. The training set contains 90% of the known links. Each result was obtained by averaging 100 implementations with independent random divisions into training and probe sets.

Algorithm	CN	AA	RA	HPI	Jaccaced
AUC	0.865	0.883	0.886	0.846	0.851
Precision	0.218	0.268	0.283	0.014	0.028
Algorithm	**LHN1**	**Salton**	**Sorenson**	**Katz**	**LHN2**
AUC	0.832	0.865	0.851	0.876	0.716
Precision	0	0.218	0.029	0.181	0.001
Algorithm	**LocalPath**	**ACT**	**Cos+**	**LRW**	**RWR**
AUC	0.880	0.790	0.873	0.903	0.908
Precision	0.183	0.135	0.072	0.112	0.165
Algorithm	**SimRank**	**SRW**	**MFI**	**PA**	**TSCN**
AUC	0.854	0.907	0.888	0.716	0.432
Precision	0.001	0.153	0.052	0.078	0.009

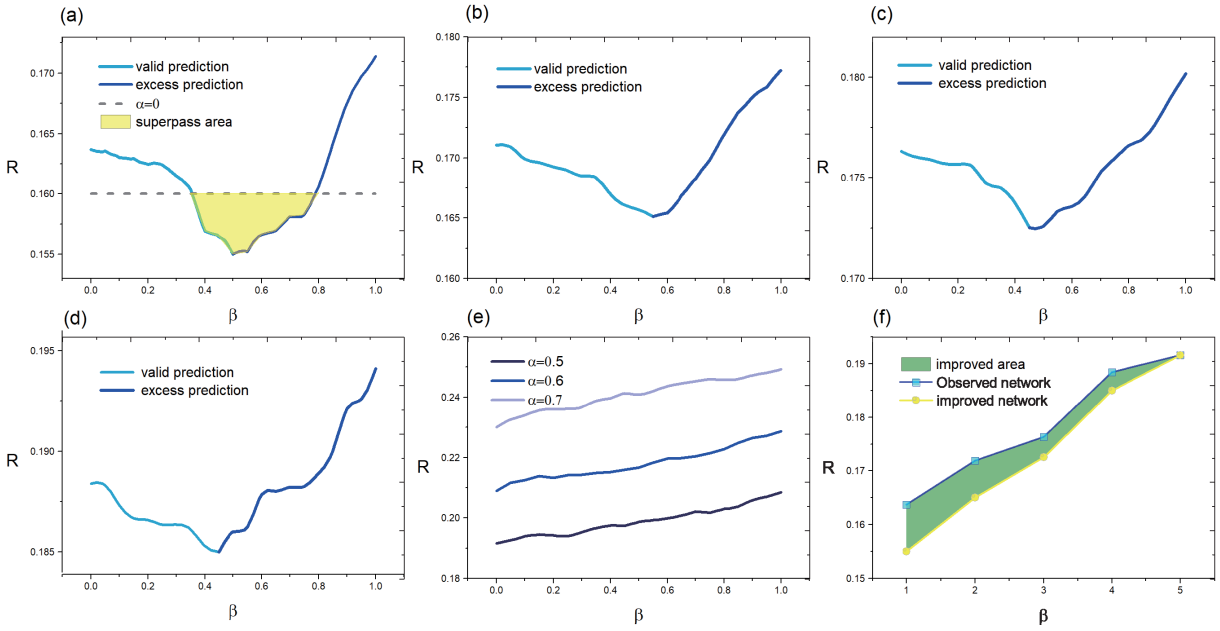

FIGURE 3. The critical attack strength coefficient f_c versus the magnitude of link prediction information β with various magnitude of missing link information α. The results are averaged over 100 independent realizations. The light grey lines represent the "valid prediction area" and the dark grey lines represent the "excessive prediction area". The dash dotted lines are the reference lines, which represent the case of complete link information $\alpha = 0$.

from 10 to 100, and the precision tends to decrease with the increasing of L [36]. Here, we set $L = 15$, which equals to the unknown links. Generally speaking, the local indices perform better than the quasi-local ones, and the global similarity indices have poor performance. The result shows that RA performs best among all the common-neighbor-based indices on the September 11^{th} hijackers network. Thus, we employ RA to predict missing links in the following experiment. Resource Allocation (RA) index [37] is motivated by the resource allocation dynamics on networks. Consider a pair of nodes, x and y, which are not directly connected. The node x can send some resource to y, with their common neighbors being transmitters. The similarity between x and y can be defined as the amount of resource y received from x. The mathematical expressions are

$$S_{xy}^{RA} = \sum_{z \in \Gamma(x) \cap \Gamma(y)} \frac{1}{k_z} \tag{2}$$

C. IMPACT OF LINK PREDICTION ON THE DISINTEGRATION EFFECT

We applied our method on the terrorists network of September 11^{th} hijackers [11] to analyze the impact of link prediction. The resource allocation (RA) link prediction algorithm [37] is chosen to predict the missing links in network, and we present the measure of network damage R on the magnitude of link prediction information β. For comparison, we also calculate the R^0 under the ideal case, i.e., complete information, $\alpha = 0$.

It is obvious that link prediction has a considerable impact on the disintegration effect. From Fig. 3(a) to Fig. 3(d), we can see that R shifts gradually to top-left with the increasing number of missing links. We find that there exists an optimal magnitude of link prediction β^*, where we can get the optimal network disintegration effect. For $\alpha = 0.1$ to $\alpha = 0.4$, R first decreases with β and we call the region $[0, \beta^*]$ "valid prediction", shown as the light blue curves. With the β increasing, then R begin to increase. Obviously, the region(β^*, β_{max}) is the "excessive prediction" because any additional predicted links will bring negative effects on the performance of network disintegration, shown as the dark blue curves. It is important to note that, when α is large enough, for example, $\alpha \geq 0.5$, there is no "valid prediction area", thus $\beta^* = 0$, shown in the Fig. 3(e). It Indicates that, if more than half links are missing, link prediction will have a negative effect on the network disintegration performance. Facing a large amount of missing information, link prediction cannot capture valid structural similarity information based on the observation networks in order to make a correct prediction. As a result, the prediction accuracy is very low, any adding links will bring more noise [38].

Moreover, we observe that, with missing link information $\alpha = 0.1$, there exists an area in which the disintegration effect of our method is even better than the ideal case, R^0, shown as the grey dash dotted lines. We refer to this phenomenon as the "comic effect" of link prediction. It can be explained that the link prediction amplifies the heterogeneity of node importance and reshape the network structure like drawing an exaggerated and characteristic comic. In fact, in the view of network disintegration, we concern the structure recover rather than the links recover. as a tool to capture the network structural similarity, the links added by link prediction have

TABLE 2. The precision of top 10 terrorists versus the magnitude of missing link information. The bold name means the accuracy prediction and the italic name means a new node do not belong to the Top 10. Salem Alhazmi, Fayez Ahmed, Djamal Beghal and Zaoarias Moussaouri have the same degree, we choose Salem Alhazmi because it has a larger betweenness centrality.

Top10	$\alpha = 0.1$	$\alpha = 0.2$	$\alpha = 0.3$
Mohamed Atta	**Mohamed Atta**	**Mohamed Atta**	**Mohamed Atta**
Marwan Al Shehhi	**Marwan Al Shehhi**	**Marwan Al Shehhi**	**Marwan Al Shehhi**
Hani Hunjor	**Hani Hunjor**	Ziad Jarrah	**Hani Hunjor**
Nawaf Al hazmi	**Nawaf Al hazmi**	**Nawaf Al hazmi**	Ziad Jarrah
Essid Sami ben Khemais	Ziad Jarrah	**Essid Sami ben Khemais**	**Essid Sami ben Khemais**
Ziad Jarrah	Satam Suqami	Hani Hunjor	Satam Suqami
Abdul Aziz Al Omaari	**Abdul Aziz Al Omaari**	Satam Suqami	**Abdul Aziz Al Omaari**
Ramzi Bin al Shibh	**Ramzi Bin al Shibh**	Abdul Aziz Al Omaari	Salem Alhazmi
Satam Suqami	Essid Sami ben Khemais	*Hamza Alghamdi*	Ramzi Bin al Shibh
Salem Alhazmi	**Salem Alhazmi**	**Salem Alhazmi**	*Fayez Ahmed*
Top10	$\alpha = 0.4$	$\alpha = 0.5$	$\alpha = 0.6$
Mohamed Atta	**Mohamed Atta**	**Mohamed Atta**	**Mohamed Atta**
Marwan Al Shehhi	**Marwan Al Shehhi**	**Marwan Al Shehhi**	Nawaf Al hazmi
Hani Hunjor	Ramzi Bin al Shibh	**Hani Hunjor**	Marwan Al Shehhi
Nawaf Al hazmi	Hani Hunjor	Satam Suqami	Hani Hunjor
Essid Sami ben Khemais	**Essid Sami ben Khemais**	Ramzi Bin al Shibh	Satam Suqami
Ziad Jarrah	**Ziad Jarrah**	*Saeed Alghamdi*	*Zaoarias Moussaouri*
Abdul Aziz Al Omaari	Salem Alhazmi	*Abu Qatada*	Essid Sami ben Khemais
Ramzi Bin al Shibh	Nawaf Al hazmi	Essid Sami ben Khemais	Ziad Jarrah
Satam Suqami	**Satam Suqami**	*Ahmed Al Haznawi*	*Jerome Courtailler*
Salem Alhazmi	*Djamal Beghal*	Ziad Jarrah	*Djamal Beghal*

a strong trend to emphasize the network structure which we have known. the links may be connected to wrong nodes that we may not recover every link exactly, however, through these links added, we capture the structural characteristics which is really critical in network disintegration. This result implies that in some cases we can reconstruct the original network to improve the effect of network disintegration.

In Table. 2, we list the top 10 hijackers based on the degree centrality strategy as key nodes. We show the precision of them to see how the link prediction works in recovering their relationships. We list the recovery of key nodes with the different ratios of missing information. In the table, the bold name indicates that link prediction not only helps us find the correct important nodes, but also accurately predicts the ordering of nodes. We call it complete accurate recovery; the unconsolidated text indicates that important nodes are found through prediction, But the original order of the nodes is wrong; the italic names indicate that the important characters given by the link prediction are not among the original ten important nodes, which we call noise nodes.

We can see that when the ratio of missing information $\alpha < 0.4$, half of the key nodes can be completely recovered through link prediction, and the link prediction can always make the top three nodes right. For $\alpha = 0.1$ to $\alpha = 0.4$, the number of noise nodes is no more than three, and they are all ranked at the lower end of the table. This proves that the introduction of link prediction technology can effectively find the important nodes to improve the disintegration effect. When the ratio of missing information $\alpha = 0.5$, the link prediction can basically make the top three nodes right. As for $\alpha = 0.6$, nine of ten key nodes are not in their right place, which means adding kinks based on link prediction will be counterproductive for the network disintegration. These results show that when the link information is not complete, adding a proper number of predicted links can efficiently improve the performance of network disintegration. It is true that link prediction cannot completely recover all the missing relationships in September 11^{th} hijackers network. However, in the process of finding the right links and reconstructing the network, through calculating the structure similarity, the link connection mechanism can be better explained and we can partly put the right ranking of node importance back under the view of various disintegration strategies (i.e., degree in degree centrality, betweenness in betweenness centrality), which is really critical in network disintegration.

To explore the impact of link prediction on the disintegration effect clearly, we show the critical attack strength coefficient without link prediction $\tilde{R}$, comparing with the optimal critical attack strength coefficient R^* in Fig. 3(f). The difference between R^* and $\tilde{R}$ indicates the contribution of the additional links predicted by link prediction algorithm. We find that our method can improve the effect of network disintegration even for $\alpha \in (0, 0.5)$. It means the contribution of link prediction is efficient and stable.

D. COMPARISON WITH OTHER DISINTEGRATION STRATEGIES

As we mentioned, there are also some alternative disintegration strategies. Most researches about the network disintegration problem are concerned either with neighborhood-based centrality disintegration strategies or path-based centrality disintegration strategies. The basic disintegration strategy is the neighborhood-based centralities, such as the degree centrality strategy using in this article and local centrality strategy. Besides, some path-based structural centralities making disintegration strategies more destructive could obtain better

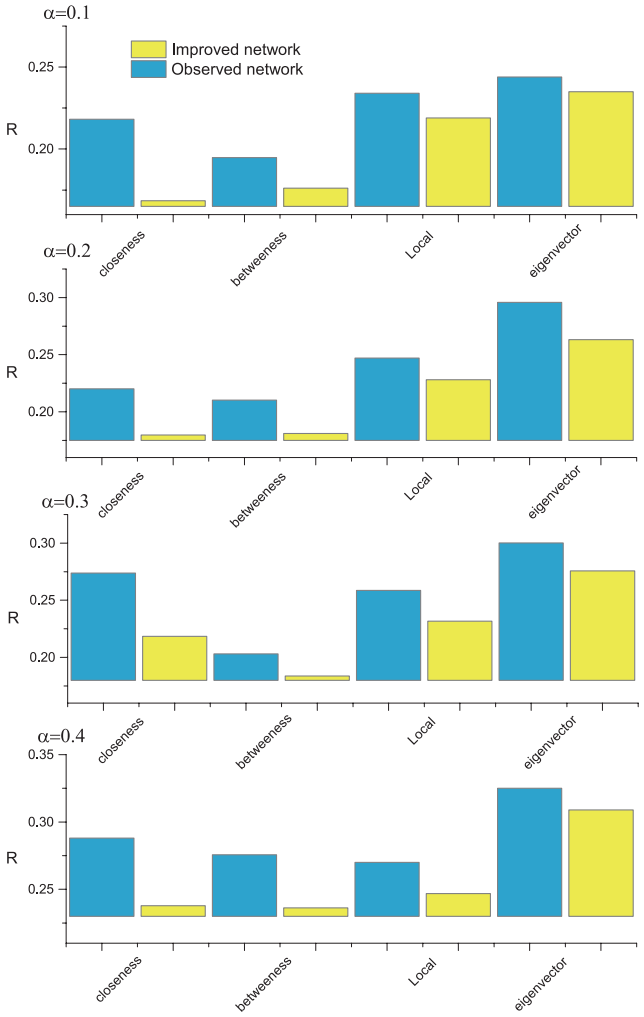

FIGURE 4. The histograms of disintegration effect with various magnitude of missing link information α. The yellow bars represent the R^* value based on the improved network reconstructed by the optimal magnitude β^*, with the assistance of link prediction. While the blue bars represent the $\tilde{R}$ value based on the observed network. Two bars form a group that calculated by the same disintegration strategy, which is marked below on the horizontal axis.

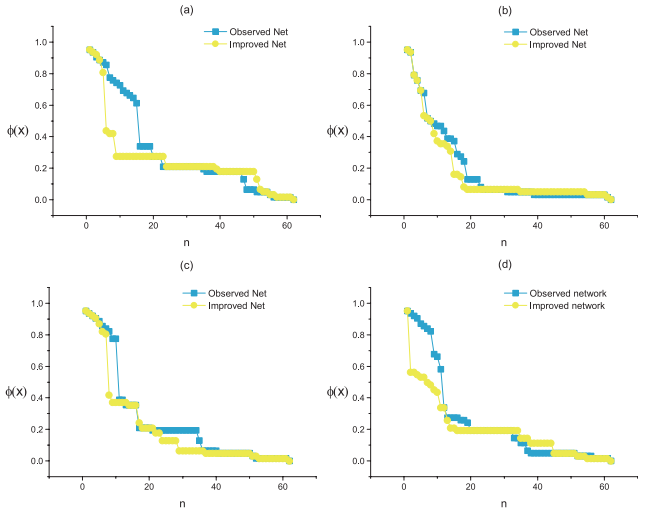

FIGURE 5. The relative size of the largest connected component (LCC) versus four different disintegration strategies under 30% missing link information. The yellow lines represent attacking with optimal link prediction information, and the blue lines represent attacking without link prediction. The results are averaged over 100 independent realizations of link prediction.

disintegration effect, such as betweenness centrality [39], and closeness centrality [15]. However, they are not convenient to execute in large networks because of their high computation complexity.

In the experiment above, we employ most common ''degree centrality strategy'' to measure the important nodes, i.e., a terrorist with high degree has the potential to spread news or views to more partners directly. In fact, considering the structure of terrorist network are amorphous and distributed, the meanings of importance are wide from different aspects, and the criteria of vital nodes are diverse. For example, from the viewpoint of information dissemination, the terrorist who has the potential to spread the information faster and vaster is more vital, which should be largely affected by the paths of propagation. Therefore, a straightforward and efficient method is to directly count the distance a node from all other nodes, resulting in the closeness centrality. It inspires us to test the effectiveness of our model under various disintegration strategies. In the following experiment, we will evaluate how the efficiency of our model varies when applying different types of disintegration strategies. We applied four structural centralities as the node removal criterion of disintegration strategy as follows: local centrality strategy [40], betweenness centrality, closeness centrality and eigenvector centrality [41]. Nodes are orderly deleted according to the descending order of these structural centralities.

In Fig. 4, we show the disintegration effect versus four different disintegration strategies, with the missing link information α from 0.1 to 0.4. As we know, the lower value of R is corresponding to more destructive disintegration effect, we can observe that our model has a better destructive effect in each situation. It is worth to note that, our model is more effective by using the path-based centrality disintegration strategies, which may indicates that the recovery of information dissemination are more vital for the disintegration of the terrorist network.

Furthermore, we are also interested in the process of the network suffers a big damage until completely collapsing. The relative size of the largest connected component (LCC) means the fraction of nodes in the giant component after nodes attacks during the attacking can report this process. We denote the measure function of network performance by Γ. In detail, Γ stands for the relative size of the largest connected component (LCC) of the corresponding network. Denote by $\hat{V} \subseteq V$ the removed nodes set, and $X = [x_1, x_2, \ldots x_N]$ be the disintegration strategy, where $x_i = 1$ once $v_i \in \hat{V}$, or $x_i = 0$. Then, the disintegration effect of disintegration strategy as the degradation of network

performance after node removal should be $\Phi(X) = \Gamma(G) - \Gamma\left(\hat{G}\right) \geq 0$. The Fig.5 shows the relative size of the largest connected component (LCC) as a function of attack strength coefficient f with magnitude of missing link information 30%. We find that the yellow curves decrease faster than blue curves, especially at the beginning of the disintegration, which makes the LCC fast down below 0.5. In general, the area between two curves in each subgraph demonstrates the improvement of the effect of network disintegration due to link prediction.

IV. CONCLUSION AND DISCUSSION

The network disintegration with incomplete link information is an important and challenging problem. It is very important for us to understand the structures and functions of terrorist networks to fight with terrorism efficiently. Considering the difficulty in collecting and accessing reliable data, in this article, we propose a disintegration model based on link prediction faced the situation of incomplete information. We use link prediction to manage our strategies by detecting and recovering some missing links. In the case study of the September 11^{th} hijackers network, we find that link prediction can improve attack result and save cost. Besides, we validate our method in other different disintegration strategies, such as local centrality strategy, betweenness centrality, closeness centrality and eigenvector centrality. Moreover, we found with surprise that if the magnitude of missing link information is not too large, the effect of network disintegration with the assistance of link prediction even can be better than the case of complete link information. We called this phenomenon the ''comic effect'' of link prediction. Although, by the assistance of link prediction, our model does not recover the missing information completely, it reshapes the network just like an exaggerated but characteristic comic. As a result, the importance of the key nodes is emphasized by adding a number of predicted links. This may provide useful insights into developing effective strategies of terrorist network disintegration facing incomplete link information. There are several future research directions to pursue. Different from typical social networks, terrorist organizations tend to be more cellular and distributed. For real applications, how to obtain the optimal magnitude of link prediction information for real networks is still an open and challenging problem, as we usually do not know the portion of missing links and thus it is difficult to evaluate the algorithm's performance. Besides, our model is a particular approach based on the relationship between staffs. Lacking in this study and an interesting area for future studies, we should consider the resources, skills, tasks in network, both structure and nodes properties. In addition, the comic effect of link prediction may exist in many backgrounds, not only in the network disintegration. For example, the link prediction can not only help to improve the classification accuracy of partially labeled networks but also be used in recommender systems [42]. We believe this paper may attract extensive interest and create discussion.

APPENDIX I. THE 62 MENBERS OF THE 9/11 HIJACKERS NETWORK

TABLE 3. The names of the September 11^{th} hijackers.

1 Samir Kishk	2 Madjid Sahoune
3 Mohamed Abidi	4 Abdussattar Shaikh
5 Ossama Awadallah	6 Ahmed Khalil Ibrahim Samir
7 Fahid al sharki	8 Nizar Trabelsi
9 Nawaf Al hazmi	10 Khalid Al Mindhar
11 Mohamed Atta	12 Abdelghani Mzoudi
13 Said Bahaji	14 Mounir el motassaeq
15 Mamoun Darkazanali	16 Mamduh Mahmud Salim
17 Essid Sami ben Khemais	18 Hyder Abu Doha
19 Wail Al Shehhi	20 Waleed Al Shehhi
21 Raed Hijazi	22Nabil al Marabh
23 Majed Moqed	24 Faisal al salmi
25 Seifallah ben hassine	26 Mehdi Khammoun
27 Ahmed Ressam	28 Lased Ben Heni
29 Mohamed Bensakhria	30 Abu Zubaida
31 Abu Walid	32 Kamel Dauod
33 Jerome Courtailler	34 David Courtailler
35 Mohamed Belfas	36 Agus Badim
37 Marwan Al Shehhi	38 Zakariya Essabar
39 Salem Alhazmi	40 Ahmed Alghamdi
41 Ahmed Al Haznawi	42 Ziad Jarrah
43 Mohand Al Shehhi	44 Hamza Alghamdi
45 Saeed Alghamdi	46 Ahmed alnami
47 Mustafa Ahmed Al Hissaw	48 Fayez Ahmed
49 Abdul Aziz Al Omaari	50 Satam Suqami
51 Lotfi Raissi	52 Hani Hunjor
53 Rayed Mohammed Abdullah	54 Bandar Alhazmi
55 Imdad Eddin Barakat Yarkas	56 Ramzi Bin al Shibh
57 Zaoarias Moussaouri	58 Abu Qatada
59 Essoussi Laaroussi	60 Tare Maaroufi
61 Djamal Beghal	62 Jean Marc Grandvisir

REFERENCES

[1] J. Raab and H. B. Milward, ''Dark networks as problems,'' *J. Public Admin. Res. Theory*, vol. 13, no. 4, pp. 413–439, 2003.

[2] A. Sinha, K. Mitchell, and D. Medhi, ''Network game traffic: A broadband access perspective,'' *Comput. Netw.*, vol. 49, no. 1, pp. 71–83, 2005.

[3] K. M. Carley, ''Destabilization of covert networks,'' *Comput. Math. Org. Theory*, vol. 2, no. 1, pp. 51–66, 2006.

[4] M. Kenney, ''From Pablo to Osama: Trafficking and terrorist networks, government bureaucracies, and competitive adaptation,'' *Terrorism Political Violence*, vol. 19, no. 4, pp. 623–624, 2008.

[5] J. Arquilla, D. Ronfeldt, and M. Zanini, ''Networks, netwar, and information-age terrorism,'' *Current History*, vol. 99, no. 636, pp. 75–111, 2001.

[6] M. Sageman, ''Understanding terror networks,'' *Int. J. Emergency Mental Health*, vol. 7, no. 1, pp. 5–8, 2005.

[7] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, ''Survey on threats and attacks on mobile networks,'' *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[8] S. Wasserman and K. Faust, ''Social network analysis: Methods and applications,'' *Contemp. Sociol.*, vol. 91, no. 435, pp. 219–220, 1995.

[9] H. Tu, J. Allanach, S. Singh, K. R. Pattipati, and P. Willett, ''Information integration via hierarchical and hybrid Bayesian networks,'' *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 36, no. 1, pp. 19–33, Jan. 2006.

[10] Y. Kim, T. Y. Choi, T. Yan, and K. Dooley, ''Structural investigation of supply networks: A social network analysis approach,'' *J. Oper. Manage.*, vol. 29, no. 3, pp. 194–211, 2011.

[11] V. Krebs, ''Mapping networks of terrorist cells,'' *Connections*, vol. 24, no. 3, pp. 43–52, 2002.

[12] I. C. Moon and K. M. Carley, ''Modeling and simulating terrorist networks in social and geospatial dimensions,'' *IEEE Intell. Syst.*, vol. 22, no. 5, pp. 40–49, Sep. 2007.

[13] A. Bavelas, ''A mathematical model for group structures,'' *Human Org.*, vol. 7, no. 3, pp. 16–30, 1948.

[14] L. C. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, vol. 40, no. 1, pp. 35–41, 1977.
[15] L. C. Freeman, "Centrality in social networks conceptual clarification," *Social Netw.*, vol. 1, no. 3, pp. 215–239, 1979.
[16] D. M. A. Hussain, "Terrorist networks analysis through argument driven hypotheses model," in *Proc. 2nd Int. Conf. Availab., Rel. Secur.*, Apr. 2007, pp. 480–492.
[17] U. K. Wiil, N. Memon, and P. Karampelas, "Notice of violation of IEEE publication principles detecting new trends in terrorist networks," in *Proc. Int. Conf. Adv. Social Netw. Anal. Mining*, 2010, pp. 435–440.
[18] N. Memon, J. D. Farley, D. L. Hicks, and T. Rosenorn, *Mathematical Methods in Counterterrorism*. Vienna, Austria: Springer, 2009.
[19] N. Memon, H. L. Larsen, N. Harkiolakis, and N. Harkiolakis, "Retracted: Detecting hidden hierarchy in terrorist networks: Some case studies," in *Proc. IEEE ISI Int. Workshops Intell. Secur. Inform.*, 2008, pp. 477–489.
[20] K. M. Carley, "Estimating vulnerabilities in large covert networks using multi-level data," in *Proc. Int. Symp. Command Control Res. Technol.*, San Diego, CA, USA, vol. 1, Jun. 2004.
[21] V. A. Lefebvre and J. D. Farley, "The torturer's dilemma: A theoretical analysis of the societal consequences of torturing terrorist suspects," *Stud. Conflict Terrorism*, vol. 30, no. 7, pp. 635–646, 2007.
[22] F. Morone and H. A. Makse, "Influence maximization in complex networks through optimal percolation," *Nature*, vol. 524, no. 7563, pp. 65–68, 2015.
[23] Y. Chen, G. Paul, S. Havlin, F. Liljeros, and H. E. Stanley, "Finding a better immunization strategy," *Phys. Rev. Lett.*, vol. 101, no. 5, 2008, Art. no. 058701.
[24] C. M. Schneider, A. A. Moreira, J. S. Andrade, Jr., S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proc. Nat. Acad. Sci. USA*, vol. 108, no. 10, pp. 3838–3841, 2011.
[25] R. M. Adler, "A dynamic social network software platform for counter-terrorism decision support," in *Proc. IEEE Intell. Secur. Inform.*, May 2007, pp. 47–54.
[26] Z. Li, D.-Y. Sun, S.-Q. Guo, and B. Li, "Detecting key individuals in terrorist network based on fanp model," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining*, Aug. 2014, pp. 724–727.
[27] L. da Fontoura Costa *et al.*, "Analyzing and modeling real-world phenomena with complex networks: A survey of applications," *Adv. Phys.*, vol. 60, no. 3, pp. 329–412, 2011.
[28] L. Lü and T. Zhou, "Link prediction in complex networks: A survey," *Phys. A, Stat. Mech. Appl.*, vol. 390, no. 6, pp. 1150–1170, 2011.
[29] J. Shen *et al.*, "Predicting protein–protein interactions based only on sequences information," *Proc. Nat. Acad. Sci. USA*, vol. 104, no. 11, pp. 4337–4341, 2007.
[30] J. Menche *et al.*, "Uncovering disease-disease relationships through the incomplete interactome," *Science*, vol. 347, no. 6224, 2015, Art. no. 1257601.
[31] L. Lü, L. Pan, T. Zhou, Y.-C. Zhang, and H. E. Stanley, "Toward link predictability of complex networks," *Proc. Nat. Acad. Sci. USA*, vol. 112, no. 8, pp. 2325–2330, 2015.
[32] B. Chen, Y. Hua, Y. Yuan, and Y. Jin, "Link prediction on directed networks based on AUC optimization," *IEEE Access*, vol. 6, pp. 28122–28136, 2018.
[33] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 65, no. 1, p. 056109, 2002.
[34] H. J. Herrmann, C. M. Schneider, A. A. Moreira, J. S. Andrade, Jr., and S. Havlin, "Onion-like network topology enhances robustness against malicious attacks," *J. Stat. Mech. Theory Exp.*, vol. 1, no. 1, p. 01027, 2011.
[35] R. Lambiotte, J. C. Delvenne, and M. Barahona, "Random walks, Markov processes and the multiscale modular organization of complex networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 1, no. 2, pp. 76–90, Jul. 2014.
[36] J. L. Herlocker, J. A. Konstan, L. G. Terveen, and J. T. Riedl, "Evaluating collaborative filtering recommender systems," *ACM Trans. Inf. Syst.*, vol. 22, no. 1, pp. 5–53, 2004.
[37] T. Zhou, L. Lü, and Y.-C. Zhang, "Predicting missing links via local information," *Eur. Phys. J. B, Condens. Matter*, vol. 71, no. 4, pp. 623–630, 2009.
[38] W. Liu and L. Lü, "Link prediction based on local random walk," *Europhys. Lett.*, vol. 89, no. 2, 2010, Art. no. 58007.
[39] M. Bellingeri, D. Cassi, and S. Vincenzi, "Efficiency of attack strategies on complex model and real-world networks," *Phys. A, Stat. Mech. Appl.*, vol. 414, no. 10, pp. 174–180, 2014.
[40] D. Chena, L. Lü, M.-S. Shang, Y.-C. Zhang, and T. Zhou, "Identifying influential nodes in complex networks," *Phys. A, Stat. Mech. Appl.*, vol. 391, no. 4, pp. 1777–1787, 2012.
[41] P. Bonacich, "Factoring and weighting approaches to status scores and clique identification," *J. Math. Sociol.*, vol. 2, no. 1, pp. 113–120, 1972.
[42] L. Lü, M. Medo, C. H. Yeung, Y.-C. Zhang, Z.-K. Zhang, and T. Zhou, "Recommender systems," *Phys. Rep.*, vol. 519, no. 1, pp. 1–49, 2012.

ZHENDONG SU received the B.S. degree in command automation from the Army Academy of Artillery and Air Defense, Hefei, China, in 1996, and the M.S. degree in equipment support from the Academy of Armored Forces Engineering Institute, Beijing, China, in 1999. He is currently pursuing the Ph.D. degree in management science and engineering from the University of Science and Technology of China, Hefei.

His current research interests include high-performance computing, complex networks, and parallel management and control for complex systems.

KAIJUN REN received the B.S. degree in applied mathematics and the M.S. and Ph.D. degrees in computer science from the National University of Defense Technology, Changsha, China, in 1998, 2003, and 2008, respectively.

He is currently a Professor with the College of Computer and the College of Meteorology and Oceanology, National University of Defense Technology. His current research interests include high-performance computing, cloud computing, big data, complex systems theory, and their inter-disciplinary applications in ocean science and meteorology areas.

RUOYUN ZHANG received the B.S. degree in command automation and the M.S. degree in higher education from the National University of Defense Technology, Changsha, China, in 2014 and 2016, respectively, where she is currently pursuing the Ph.D. degree in management science and engineering.

Her current research interests include complex networks and threaten networks, especially the structural robustness of complex networks.

SUO-YI TAN received the B.S., M.S., and Ph.D. degrees in management science and engineering from the National University of Defense Technology, Changsha, China, in 2012, 2014, and 2018, respectively.

From 2016 to 2017, he was a Visiting Ph.D. Student with the Center for Polymer Studies, Boston University, Boston, MA, USA. He is currently a Lecturer with the College of Systems Engineering, National University of Defense Technology. His current research interests include link prediction and complex networks, especially the structural robustness of complex networks.